UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/766,142	01/19/2001	William D. Evans	D/A0A87	1295

7590 08/02/2005

Patent Documentation Center
Xerox Corporation
Xerox Square 20th Floor
100 Clinton Ave. S.
Rochester, NY 14644

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/766,142	EVANS, WILLIAM D.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15-29,35,37,38,41 and 42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-29,35,37,38,41 and 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claim 15-29, 35, 37, 38, 41, and 42 are pending in this office action.

Rejections

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

3. Claims 15-29, 35, 37, 38, 41, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carter (U.S. Patent No. 5,787,175) in view of Follendore, III (U.S. Patent No. 6,011,847), and further in view of Tada et al. (U.S. Patent No. 6,178,422).

Regarding claim 15, Carter teaches a secure content object, comprising:

- Encrypting the electronic document using a document encryption key**, wherein access to the electronic document is available to a first set of authorized users** (fig. 6, ref. num 112 and col. 13, lines 4-17);
- A **first** multi-key encryption table for use in a multi-key encryption method **associated with the electronic document**, the **first** table comprising at least one multi-key encryption component **associated with each authorized user in**

the first set (fig. 6, ref. num 114, 116, and 118 and col. 13, line 18 through col. 14, line 22);

- A user interface device comprising unencrypted information for identifying the electronic document and an interactive element for enabling a user to input a user authorization for access to at least a portion of the encrypted electronic document, for inputting the user authorization to a decryption engine using the multi-key encryption method for combining the user authorization with each of the multi-key components in the **first** multi-key encryption key table to decrypt the encrypted header, and **for combining the user authorization with each of the stored multi-key components in the second multi-key encryption key table to decrypt an annotation** (fig. 9, ref. num 152 and col. 16, lines 16-29);
- **Wherein upon a valid decryption of the annotation indicates the correct annotation encryption key has been found and the user is an authorized user** (col. 17, lines 5-11).

Carter does not teach an encrypted header, a plurality of dummy encryption components, **a plurality of annotations generated by an annotation author, wherein access to the annotations is available to the users designated by the annotation author as having access to the plurality of annotation, a second multi-key encryption table comprising at least one multi-key component associated with each authorized annotation user**, and upon a valid decryption of the encrypted header, decrypting the portion of the encrypted electronic document.

Follendore, III teaches an encrypted header comprising information pertaining to the electronic document (fig. 2, ref. num 224 and col. 1, lines 22-25), a plurality of dummy encryption components, wherein the multi-key encryption table includes no information that may identify a user of the electronic document (col. 8, line 51 through col. 9, line 7), upon a valid decryption of the encrypted header, decrypting the portion of the encrypted electronic document (fig. 2, ref. num 242).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating an encrypted header comprising information pertaining to the electronic document and upon valid decryption of the header, decrypting the encrypted electronic document, and generating a plurality of dummy encryption components, wherein the table includes no information identifying a user or the document, as taught by Follendore, III, with the object of Carter. It would have been obvious for such modifications because a header defines the data portion of the document. When the header is decrypted, a decryption key contained in the header for decrypting the document allows the key to be transmitted safely. Also, the dummy data provides random data to include that will make the length of the data fields the same size; this aids in the encryption process (see col. 8, line 51 through col. 9, line 7 of Follendore, III).

The combination of Carter as modified by Follendore, III still does not teach **a plurality of annotations generated by an annotation author, wherein access to the**

plurality of annotations is available to the users designated by the annotation author as having access to the plurality of annotation and a **second multi-key encryption table comprising at least one multi-key component associated with each authorized annotation user**.

Tada et al. teaches **a plurality of annotations generated by an annotation author, the plurality of annotations having been encrypted with an annotation encryption key, wherein access to the plurality of annotations is available to the authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotation** (col. 5, lines 37-65 and col. 6, lines 20-24); and a **second multi-key encryption table for use in a multi-key encryption method associated with the plurality of annotations, the second table comprising at least one multi-key component associated with each authorized annotation user** (fig. 2, 3, and 8).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a multi-key table containing specific users that are allowed to access the annotations provided by the author of the annotations, as taught by Tada et al., with the object of Carter/Follendore, III. It would have been obvious for such modifications because user groups circumvent the problems of having to modify a document for every user, and allows a document to specify which users can access the document (see col. 2, lines 8-14 and 31-38 of Tada et al.).

Regarding claim 16, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates that the document encryption key has been found (see fig. 2, ref. num 230, 232, and 234 Follendore, III).

Regarding claim 17, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the electronic document comprises content information that is formatted based on an object language having a set of formatting rules (see col. 8, lines 17-26 of Carter).

Regarding claim 18, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the user interface device comprises a second electronic document (see col. 5, lines 34-39 of Follendore, III).

Regarding claim 19, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the information pertaining to the electronic document comprises a user permission table for access to all or portions of the electronic document and wherein only those permitted portions of the electronic document are decrypted (see col. 8, lines 51-59 of Carter).

Regarding claim 20, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the encrypted header and the encrypted electronic document are encrypted using different encryption keys and wherein the multi-key encryption table includes at least one multi-key component for each encryption key (see fig. 4, ref. num 428, 430, 432, and 434 of Follendore, III).

Regarding claim 21, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the encrypted header further comprises a fingerprint for identifying some predefined aspect of the electronic document (see fig. 2, ref. num 230, 232, and 234 of Follendore, III).

Regarding claim 22, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the electronic document comprises a plurality of individual electronic documents and the encrypted header comprises information pertaining to each of the individual electronic documents (see col. 9, lines 44-49 of Carter).

Regarding claim 23, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the information pertaining to the electronic document comprises a user permission table setting forth access to all or portions of each of the individual electronic documents and wherein only those permitted portions of the authorized electronic document are decrypted (see col. 8, lines 51-59 of Carter).

Regarding claim 24, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the content information is selected from the group consisting of text, graphics, equations, tables, spreadsheets, pictures, video files, audio files, multimedia files and binary data of unknown format (see col. 8, lines 17-26 of Carter).

Regarding claim 25, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the object language comprises Adobe Acrobat (see col. 8, lines 17-26 of Carter).

Regarding claim 26, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the object language comprises a language which interprets Microsoft Word documents (see col. 8, lines 17-26 of Carter).

Regarding claim 27, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the header encryption key has been found (see fig. 2, ref. num 230, 232, and 234 Follendore, III); and wherein the encrypted electronic document includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker

indicates the document encryption key has been found (see fig. 2, ref. num 234, 236, and 238 of Follendore, III).

Regarding claim 28, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the electronic document includes a document ID and wherein the document encryption key includes a combination of the document ID, the user information and the multi-key components, for each authorized user (see fig. 4, ref. num 92 and 96 and col. 13, line 63 through col. 14, line 5 of Carter).

Regarding claim 29, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the electronic document comprises a first electronic document and an annotation associated therewith, wherein the annotation is encrypted using an encryption key associated with a user generating the annotation (see fig. 10, ref. num 176, 180 and 182 and col. 20, lines 51-65 of Carter); and wherein the encrypted header includes information pertaining to the first electronic document and the annotation (see col. 9, lines 56-61 of Follendore, III).

Regarding claim 35, Carter teaches a method for creating a document with secure annotations, comprising:

- Providing an electronic document, wherein access to the electronic document is available to a first set of users (fig. 4, ref. num 54,90);

- **Responsive to a first user from the first set of users,** generating a plurality of annotations pertaining to the electronic document using the document language (fig. 10, ref. num 176);
- Encrypting each annotation using an annotation encryption key associated with **the first** user generating the particular annotation, wherein access to an encrypted annotation is available to **authorized** users having access to the respective annotation encryption key (fig. 10, ref. num 180 and 182 and col. 20, lines 51-65);

  For each annotation encryption key:
- Generating a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component (fig. 6, ref. num 114, 116, and 118 and col. 13, line 18 through col. 14, line 22);
- Providing a user interface for enabling a user to input a user authorization for access to at least a portion of an encrypted annotation (fig. 9, ref. num 152 and col. 16, lines 16-29);
- **Wherein, responsive to an input user authorization,** combining the **input** user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the annotation, wherein valid decryption of the annotation indicates the correct annotation encryption key has been found (fig. 11, ref. num 192); and

- Access to the encrypted electronic document is available to the first set of users and access to the encrypted annotations in the separate file is provided only to **authorized** users (fig. 11, ref. num 192).

Carter does not teach **associating the plurality of annotations with the first user, designating which users in the first set of users are authorized users have access to the plurality of annotations, associating with each authorized user having been designated by the first user as having access to the annotation**, concatenating the plurality of encrypted annotations in a second electronic document, and merging the second electronic document and the encrypted electronic document into a third electronic document.

Follendore, III teaches concatenating the plurality of encrypted annotations in a second electronic document (fig. 2, ref. num 224), and merging the second electronic document and the encrypted electronic document into a third electronic document (fig. 2, ref. num 222 and 224 contained within 218).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine concatenating the annotations in a second document and merging the second electronic document and the encrypted electronic document into a third electronic document, as taught by Follendore, III, with the method of Carter. It would have been obvious for such modifications because the annotations can become

many for only one file. By combining the annotations into their own electronic document, they can be handled on their own with their own keys separate from the electronic document.

The combination of Carter as modified by Follendore, III still does not teach **associating the plurality of annotations with the first user, designating which users in the first set of users are authorized users have access to the plurality of annotations, associated with each authorized user having been designated by the first user as having access to the annotation**.

Tada et al. teaches **associating the plurality of annotations with the first user, designating which users in the first set of users are authorized users have access to the plurality of annotations, associated with each authorized user having been designated by the first user as having access to the annotation** (fig. 2, 3, and 8, and col. 5, lines 37-65 and col. 6, lines 20-24).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine associating the authorized users for viewing the annotations in the table, as prescribed by the annotation author, as taught by Tada et al., with the object of Carter/Follendore, III. It would have been obvious for such modifications because user groups circumvent the problems of having to modify a

document for every user, and allows a document to specify which users can access the document (see col. 2, lines 8-14 and 31-38 of Tada et al.).

Regarding claim 37, the combination of Carter in view of Follendore, III/Tada et al. teaches further comprising the step of:

- Encrypting the first electronic document using a document encryption key, wherein access to the encrypted electronic document is provided only to **the first set of users** (see fig. 6, ref. num 112 and col. 13, lines 4-17 of Carter);
- Generating a multi-key encryption table for us in a multi-key encryption method, the table comprising at least one multi-key component **associated with each of the first set of users** (see fig. 6, ref. num 114, 116, and 118 and col. 13, line 18 through col. 14, line 22 of Carter and fig. 3 of Tada et al.);
- Generating an encrypted header comprising information pertaining to the electronic document (see fig. 2, ref. num 224 of Follendore, III);
- Providing a user interface for enabling a user to input a user authorization for access to at least a portion of the encrypted document (see fig. 9, ref. num 152 and col. 16, lines 16-29 of Carter);
- Combining the user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the encrypted header, wherein valid decryption of the encryption header indicates the document encryption key has been found (see fig. 9, ref. num 160 and 162 and col. 16, line 60 through col. 17, line 26 of Carter, and see fig. 2, ref. num 242 of Follendore, III).

Regarding claim 38, the combination of Carter in view of Follendore, III/Tada et al. teaches further comprising adding an unencrypted header identifying the generating user to each encrypted annotation (see fig. 2, ref. num 220 of Follendore, III).

Regarding claim 41, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the annotation encryption key has been found (see fig. 2, ref. num 230, 232, and 234 Follendore, III).

Regarding claim 42, the combination of Carter in view of Follendore, III/Tada et al. teaches wherein the separate file and the electronic document are stored in different locations (see col. 9, lines 37-43 of Follendore, III).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100